The HIPAA Privacy Rule and Research

Lora Kutkat
301-594-2464
kutkatl@od.nih.gov

Summary of HIPAA Privacy Rule Enforcement Activities

- Over 6000 complaints filed by end of April 2004
- Closed about 50%
  - No jurisdiction
  - No violation
  - Voluntary compliance resolved situation
- Most common issues:
  - Uses/disclosures, safeguards, access

The Privacy Rule...

Beginning on April 14, 2003, the Privacy Rule protects the privacy of certain individually identifiable health information by establishing conditions for its use and disclosure by health plans*, health care clearinghouses, and certain health care providers.

*Small health plans not required to comply until April 14, 2004.

How Might the Privacy Rule Affect Research?

Depends on:

What you do/where you work

Type of information you use, collect, receive or release

Three Rules -- Privacy Rule, Common Rule, FDA Regulations

- Privacy Rule does not replace or modify the Common Rule or FDA regulations.
- Privacy Rule is in addition to privacy protections of these regulations.
  - Applies to covered entities regardless of funding.
  - Contains standards for de-identifying health information.
  - Requires Authorization for certain uses and disclosures of certain health information.
  - Applies to decedents' information.

Who/What is Covered?

- The Privacy Rule applies to "covered entities," which includes a health care provider who transmits health information electronically in connection with a transaction for which the Secretary has adopted standards.

  Example: a physician who electronically bills for services

- Protected Health Information (PHI) =

  Covered Entity + Health information + Identifier

  Transmitted or maintained in any form (paper, oral, electronic, forms, web-based, etc.).

  Decedents' information included.

Sources of PHI

Research Study Database

Study ID	Last Name	Zip Code	Age	DBP	SBP	Heart Rate
001	Doe	20892	41	80	120	60
002	Smith	20601	35	90	140	78
003	Jacob	32548	38	81	130	70
004	Cho	56482	45	85	120	67

Checklist:

Covered Entity?

Yes **No**

Individually Identifiable?

Yes **No**

Health Information*?

Yes **No**

*PHI includes demographic information about an individual. See the definitions of *health information* and *individually identifiable health information* at 45 CFR 160.103.

Key Point about Research

- For research, the Privacy Rule permits covered entities to use and disclose PHI for research conducted:
  - with individual authorization, **or**
  - without individual authorization under limited circumstances.

Authorizations for Research

- Must be for a specific research study – Authorization for future, unspecified research is NOT permitted but Authorization may be obtained to permit the use or disclosure of PHI to create or maintain a repository or database.
- Different from, but may be combined with, informed consent.
- Review/approval by IRB/Privacy Board NOT needed under Privacy Rule. (But other regulations would require IRB review when combined with informed consent documents.)
- Must contain “core elements” & “required statements,” and a signed copy must be given to the individual.
- Research Authorizations need not expire, but this must be stated.

Elements of an Authorization to Use or Disclose PHI

Core Elements (signified by ■)

- ■ Description of PHI to be used or disclosed
- ■ Person(s) authorized to make the requested use or disclosure.
- ■ Person(s) to whom the covered entity may disclose PHI.
- ■ Each purpose for the use or disclosure.
- ■ Expiration date or event* (e.g. “end of the research study” or “none”).

Statements (signified by ▲)

- ▲ Right to revoke Authorization plus exceptions and process.
- ▲ Ability/Inability to condition treatment, payment, or enrollment/eligibility for benefits on Authorization.
- ▲ PHI may no longer be protected by Privacy Rule once it is disclosed by the covered entity.

_____

■ Participant Signature ■ Date

The authorization must be written in plain language, and the covered entity must provide the individual with a copy of the signed Authorization.

Does the Privacy Rule specify who must develop the Authorization form?

No. The Privacy Rule does not specify who may draft the Authorization, so a researcher could draft it. However, in order to comply with the Privacy Rule, an Authorization must be written in plain language and contain the core elements and required statements specified at section 164.508 of the Privacy Rule. A covered entity may disclose PHI as specified in a valid Authorization that has been created by another covered entity or a third party, such as a researcher.

Q&A from Clinical Research Fact Sheet

When a covered entity chooses to combine the Authorization with the informed consent document for a research study, can the compound document cross-reference required elements for both permissions (i.e., to minimize redundant language)?

Yes. The Privacy Rule permits the compound Authorization to cross-reference relevant sections of an informed consent document, so long as the compound document includes the core elements and statements required by section 164.508(c). In addition, under the HHS and FDA Protection of Human Subjects Regulations, all of the required elements for informed consent would need to be in included in the informed consent document, unless an IRB alters or waives the requirements.

Use or Disclosure of PHI *Without* Authorization

Covered entities do not always need to get Authorization for research-related activities.

1. De-identify PHI.
2. Limited Data Set with Data Use Agreement.
3. IRB or Privacy Board waiver of Authorization requirement.
4. Activity preparatory to research.
5. Research is on decedents' information.
6. Research qualifies for the Transition Provisions.

De-identified Health Information

- Completely de-identified information (18 elements removed) and no knowledge that remaining information can (alone or in combination with other information) identify the individual.

OR

- Statistically “de-identified” information where a qualified statistician determines that there is a “very small” risk that the information could be used, alone or in combination with other reasonably available information, to identify the individual and documents the methods and results of the analysis.

Removal of These Identifiers* Makes Information De-identified

- Names
- Geographic info (including city and ZIP)
- Elements of dates (except year), ages over 89 years
- Telephone #s
- Fax #s
- E-mail address
- Social Security #
- Medical record, prescription #s
- Health plan beneficiary #s
- Account #s
- Certificate/license #s
- VIN and Serial #s, license plate #s
- Device identifiers, serial #s
- Web URLs
- IP address #s
- Biometric identifiers (finger prints)
- Full face, comparable photo images
- Unique identifying #s

*See 45 CFR 164.514(b)(2)(i) for a complete list.
Health information is de-identified if the above identifiers of the individual or of relatives, employers, or household members of the individuals are removed and the covered entity has no actual knowledge that remaining information can be used, alone or in combination with other information, to identify the individual.

Does "Unique Identifier" Include a Re-identification Code?

- A covered entity may assign a code to allow information de-identified under the Privacy Rule to be re-identified by the covered entity, as long as:
  - The code is not derived from or related to information about the individual.
  - The code is not otherwise capable of being translated to identify the individual. And
  - The covered entity does not use or disclose the code for any other purpose, and does not disclose the mechanism for re-identification.
- Disclosure of a code or other means of record identification designed to enable coded (or otherwise de-identified information) to be re-identified is a disclosure of PHI. And
- If de-identified information is re-identified, a covered entity must use or disclose such re-identified information in accordance with the Privacy Rule.

Q&A from Repository/Database Fact Sheet

Are an individual's initials considered to be identifiers under the Privacy Rule?

Yes, because an individual's name is an identifier and initials are derived from the individual's name, initials are considered identifiers under the Privacy Rule. Thus, for information to be de-identified using the safe harbor method of the Privacy Rule, an individual's initials must be stripped from the information. However, it may be possible for initials to remain as part of de-identified information if the statistical method for de-identification at section 164.514(b)(1) allows it.

A researcher requests data that assigns a code derived from the last four digits of the social security number. This code is necessary to link individual records from different data sources. The data contain none of the other listed HIPAA identifiers at section 164.514(b)(2). Are the data de-identified under the Privacy Rule?

No. Under the Privacy Rule, a de-identified data set may not contain unique identifying codes, except for codes that have not been derived from or do not relate to information about the individual and that cannot be translated so as to identify the individual. A code derived from part of a social security number, medical record number, or other identifier would not meet this test.

Limited Data Set with Data Use Agreement

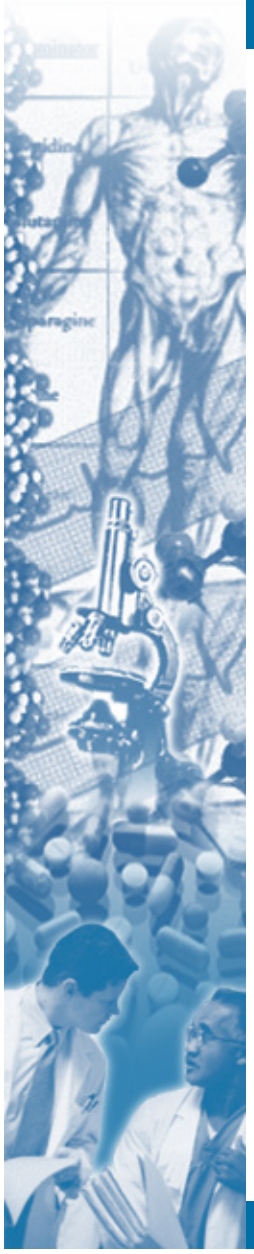
- The Privacy Rule permits limited types of identifiers to be released for research with health information (referred to as a Limited Data Set).

- Limited Data Sets can only be used and released in accordance with a Data Use Agreement between the covered entity and the recipient.

Limited Data Set with Data Use Agreement

- The Limited Data Set CAN contain
  - Elements of Dates.
  - City, town, state, and ZIP.
  - Other unique identifiers, characteristics and codes not previously listed as direct identifiers (previous slide).

MEDICAL CHART
Individually Identifiable



Record No.
0012345

Date of Birth
12/05/60

Name
Jane Doe

Gender
Female

Address
1234 NIH Way
Bethesda, MD 20892

Physician
Dr. Smith

Diagnosis
Bronchitis

Treatment
Zithromax

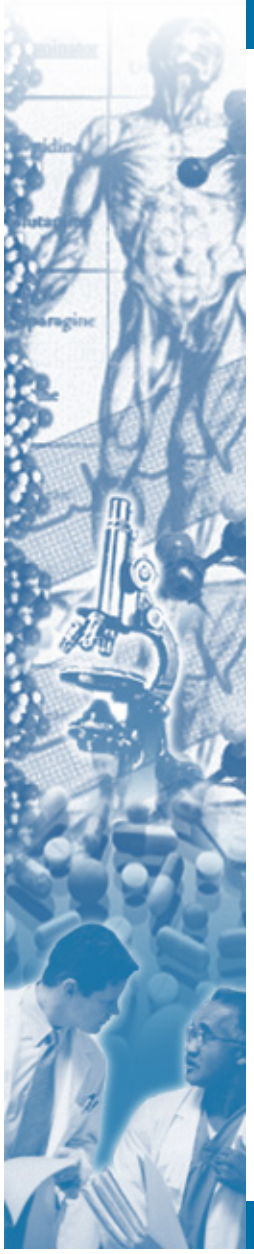
Checklist:

Covered Entity?
☑ Yes ☐ No

Individually Identifiable?
☑ Yes ☐ No

Health Information?
☑ Yes ☐ No

MEDICAL CHART
Individually Identifiable Limited Data Set



Record No.

Date of Birth

12/05/60

Name

Gender

Female

Address

Bethesda, MD 20892

Physician

Dr. Smith

Diagnosis

Bronchitis

Treatment

Zithromax

Checklist:

Individually Identifiable?

☑ Yes ☐ No

Health Information?

☑ Yes ☐ No

Data Use Agreement

☑ Yes ☐ No

MEDICAL CHART
De-identified

Record No.

Date of Birth

Name

Gender

Female

Address

Physician

Dr. Smith

Diagnosis

Bronchitis

Treatment

Zithromax

Checklist:

18 identifiers?

☐ Yes ☑ No

Knowledge of identifiability?*

☐ Yes ☑ No

Health Information?

☑ Yes ☐ No

*If the covered entity has actual knowledge that remaining information can be used to identify the individual, the information is considered individually identifiable, and therefore, generally is PHI.

Q&A from Repository/Database Fact Sheet

Does the Privacy Rule permit a covered entity to de-identify health information or create a limited data set without obtaining Authorization, waiver of the Authorization requirement from an IRB or Privacy Board, or representations for reviews preparatory to research?

Yes. In the Privacy Rule, creating de-identified health information or a limited data set is a health care operation of the covered entity, and thus, does not require the covered entity to obtain an individual's Authorization, a waiver of the Authorization requirement, or representations for reviews preparatory to research. If a business associate is hired by a covered entity to de-identify health information or create a limited data set, such activity must be conducted in accordance with the business associate requirements at sections 164.502(e) and 164.504(e).

Can a limited data set include the geographic subdivision code with the five-digit ZIP code (or a nine-digit ZIP code)?

Yes, the limited data set may include the five-digit or nine-digit ZIP code plus any other geographic subdivision, such as state, county, city, precinct, and their equivalent geocodes, except for street name or street address or post office box.

Waiver of Authorization

- A covered entity is permitted to use or disclose PHI for research when it obtains required documentation of the IRB or Privacy Board approval of a waiver of Authorization.

- Note: A covered entity is also permitted to use or disclose PHI for research when it obtains an altered Authorization under the Privacy Rule and required documentation of the IRB or Privacy Board approval of an alteration of Authorization.

IRB/Privacy Board Criteria for Waiving or Altering Authorization

	Yes	No
1. The use or disclosure involves no more than minimal risk because of an adequate plan/assurance:	☑	☐
a. To protect identifiers from improper use or disclosure.	☑	☐
b. To destroy identifiers at earliest opportunity, consistent with the conduct of the research.	☑	☐
c. That PHI will not be inappropriately reused or disclosed.	☑	☐
2. The research could not practicably be conducted without the waiver or alteration.	☑	☐
3. The research could not practicably be conducted without access to and use of PHI.	☑	☐

Signature of IRB/Privacy Board Chair (or Designee) Date

Required Documentation of a Waiver or Alteration of Authorization Includes:

1. Identity of the approving IRB or Privacy Board.
2. Date on which the waiver or alteration was approved.
3. A statement that the IRB or Privacy Board has determined that all of the specified criteria for a waiver or an alteration were met.
4. A brief description of the PHI for which use or access has been determined by the IRB or Privacy Board to be necessary in connection with the specific research activity.
5. A statement that the waiver or alteration was reviewed and approved under either normal or expedited review procedures.
6. The required signature of the IRB or Privacy Board chair or the chair's designee.

Preparatory to Research

Covered entity must obtain representation from the researcher that:

- The use or disclosure of PHI is sought solely to prepare a protocol or for a similar preparatory purpose.
- PHI will not be removed from the covered entity. AND
- PHI is necessary for research purposes.

What Kinds of Activities are Preparatory to Research?

- Preparing a research protocol.
- Assisting in the development of a research hypothesis.
- Aiding in research recruitment, such as identifying prospective research participants that would meet the eligibility criteria for enrollment into a research study.
- Under this provision, no PHI may be removed from the covered entity during the course of the review.

Research Recruitment

	Identify Subjects	Contact Subjects
Covered Entity	<u>Yes</u> • Preparatory to Research provision. • Need representation from workforce member.	<u>Yes</u> • Health care operation to get Authorization. • Waiver of Authorization.
Researcher (non-covered)	<u>Yes</u> • Preparatory to Research provision. • Need representation from researcher.	<u>Yes</u> • Waiver of Authorization. • As a business associate of covered entity for the health care operation.

Q&A from Clinical Research Fact Sheet

May a covered entity obtain an individual's Authorization to include his or her PHI in a clinical research recruitment database of possible research participants, such as a pre-screening log?

Yes. The Privacy Rule permits a covered entity to include an individual's PHI in a clinical research recruitment database and permit researchers access to the recruitment database, provided the individual has given his or her permission through a written Authorization. The Authorization must inform the individual of the purpose for which (e.g., for the pre-screening log for one or more clinical trials) and what PHI will be used and meet the other requirements at section 164.508 of the Privacy Rule. Alternatively, a covered entity may provide a researcher access to the PHI for reviews preparatory to research, provided the required representations are obtained. See section 164.512(i) of the Privacy Rule. Unless otherwise permitted by the Privacy Rule, a subsequent Authorization must be obtained from the individual before a covered entity may use or disclose the individual's PHI for the clinical trial itself.

"Grandfathered" Research Permissions

- Grandfathered-in under the Transition Provisions if, BEFORE April 14, 2003, covered entity obtains:
  - Participant's informed consent,
  - Waiver by an IRB of informed consent (unless informed consent sought after compliance date), or
  - Authorization or other express legal permission to use or disclose PHI for research.
  - Grandfathering ends when any change made after compliance date makes prior permission invalid.

Need a Covered Entity Account for Disclosures Made with an Alteration or Waiver of Authorization?

Yes. Where an Authorization has been waived or altered, pursuant to the process provided for by section 164.512(i) of the Privacy Rule, it is no longer an “authorization as provided in section 164.508” and thus, no longer exempt from the accounting requirements pursuant to section 164.528(a)(1)(iv).

EXAMPLE: Transition Provisions

- A study needs 1000 participants enrolled.
- 600 enrolled by signing informed consent before April 14, 2003.
- 400 will enroll after April 14, 2003.
- How many participants need to give Authorization? **400**
- How many informed consents were transitioned (presuming the informed consent was not nullified by revisions)? **600**

Accounting for Research Disclosures

	Accounting needed?	
	Yes	*No*
With a waiver of Authorization?	☑	☐
When decedent's Info?	☑	☐
When preparatory to research?	☑	☐
When public health activities, e.g. adverse event reporting?	☑	☐
With "grandfathered" permissions?	☑	☐
To the patient?	☐	☑
Before April 14, 2003 (or April 14, 2004, for small health plans)?	☐	☑

Privacy Rule Resources for Researchers

Office for Civil Rights (OCR) Web site

http://www.hhs.gov/hipaaprivacy/research/